

CLAIMS

- 1 1. A method for implementing port-based network access control at a shared media
2 port in an intermediate node, the shared media port being coupled to a plurality of client
3 nodes, the method comprising:
4 partitioning the shared media port into a plurality of logical subinterfaces, each
5 logical subinterface dedicated to providing access to a different network or subnetwork
6 accessible through the intermediate node;
7 receiving a data packet at the shared media port from a first client node;
8 associating the received data packet with a first logical subinterface in the plural-
9 ity of logical subinterfaces;
10 determining whether the first client node is authenticated to communicate over the
11 first logical subinterface's dedicated network or subnetwork; and
12 if the first client node is determined to be authenticated to communicate over the
13 first logical subinterface's dedicated network or subnetwork, forwarding the received
14 data packet over the first logical subinterface's dedicated network or subnetwork.
- 1 2. The method according to claim 1, further comprising:
2 performing at least one of dropping the received data packet or reclassifying the
3 received data packet to a different logical subinterface, if the first client node is deter-
4 mined not to be authenticated to communicate over the first logical subinterface's dedi-
5 cated network or subnetwork.
- 1 3. The method according to claim 1, wherein the first logical subinterface's dedi-
2 cated network or subnetwork is a virtual private network (VPN).
- 1 4. The method according to claim 1, wherein a logical subinterface in the plurality of
2 logical subinterfaces is dedicated to providing access to the Internet.

1 5. The method according to claim 1, wherein the step of determining whether the
2 first client node is authenticated to communicate over the first logical subinterface's
3 dedicated network or subnetwork further comprises:
4 parsing a source media access control (MAC) address from the received data
5 packet;
6 indexing an entry in a MAC filter associated with the shared media port based on
7 the value of the parsed source MAC address;
8 identifying an authentication state stored in the indexed MAC-filter entry; and
9 determining whether the first client node is authenticated to communicate over the
10 first logical subinterface's dedicated network or subnetwork based on the authentication
11 state stored in the indexed MAC-filter entry.

1 6. The method according to claim 5, wherein the MAC filter is organized as a hash
2 table.

1 7. The method according to claim 1, further comprising:
2 parsing a destination Internet Protocol (IP) address from the received data packet;
3 comparing the parsed destination IP address to one or more IP addresses stored in
4 an IP filter associated with the shared media port; and
5 if the parsed destination IP address matches an IP address stored in the IP filter,
6 forwarding the received data packet over the first logical subinterface's dedicated net-
7 work or subnetwork, even if the first client node is determined not to be authenticated to
8 communicate over that network or subnetwork.

1 8. The method according to claim 1, wherein the step of associating the received
2 data packet with the first logical subinterface, further comprises:
3 locating an entry in a routing table configured to store routing information associ-
4 ated with the received data packet; and
5 associating the received data packet with the first logical subinterface based on
6 the contents of the routing-table entry.

1 9. The method according to claim 1, further comprising:
2 receiving an authentication request from the first client node at the shared media
3 port;
4 in response to receiving the authentication request, creating a MAC filter associ-
5 ated with the shared media port if the MAC filter has not already been created;
6 copying a source MAC address stored in the received authentication request into
7 an appropriate entry in the MAC filter;
8 forwarding the received authentication request to an authentication service;
9 receiving a response from the authentication service, the response identifying an
10 authentication state associated with the first client node; and
11 storing the authentication state into the same MAC-filter entry into which the
12 source MAC address was copied.

1 10. The method according to claim 9, wherein the step of copying the source MAC
2 address into an appropriate MAC-filter entry further comprises:
3 indexing an entry in the MAC filter based on the result of applying a hash func-
4 tion to the source MAC address; and
5 storing the source MAC address at the indexed MAC-filter entry.

1 11. The method according to claim 9, wherein the received authentication request is
2 an 802.1X authentication request.

1 12. The method according to claim 9, further comprising:
2 sending an alarm message over the first logical subinterface's dedicated network
3 or subnetwork after the first client node fails to authenticate at the shared media port a
4 predetermined number of times.

1 13. The method according to claim 9, further comprising:
2 sending an alarm message over the first logical subinterface's dedicated network
3 or subnetwork after the first client node's authentication state changes from an authenti-
4 cated state to an unauthenticated or unknown state.

- 1 14. An intermediate node for implementing port-based network access control in a
2 network containing a plurality of client nodes, the intermediate node comprising:
3 a processor;
4 a shared media port for receiving a data packet from a first client node in the plu-
5 rality of client nodes; and
6 a memory adapted to store instructions for execution by the processor, at least a
7 portion of the instructions defining a network operating system configured to perform
8 the steps of:
9 partitioning the shared media port into a plurality of logical subinterfaces,
10 each logical subinterface dedicated to providing access to a different network or
11 subnetwork accessible through the intermediate node;
12 associating the data packet received from the first client node with a first
13 logical subinterface in the plurality of logical subinterfaces;
14 determining whether the first client node is authenticated to communicate
15 over the network or subnetwork to which the first logical subinterface provides
16 dedicated access; and
17 forwarding the received data packet over the first logical subinterface's
18 dedicated network or subnetwork only if the first client node is determined to be
19 authenticated to communicate over that network or subnetwork.
- 1 15. The intermediate node according to claim 14, wherein:
2 the memory is further adapted to store a MAC filter containing one or more en-
3 tries configured to store at least a MAC address and an authentication state, and
4 the network operating system is further configured to perform the steps:
5 receiving an authentication request from the first client node at the
6 shared media port;
7 copying a source MAC address stored in the received authentica-
8 tion request into an appropriate entry in the MAC filter;
9 forwarding the received authentication request to an authentication
10 service;

11 receiving a response from the authentication service, the response
12 identifying an authentication state associated with the first client node; and
13 storing the authentication state into the same MAC-filter entry into
14 which the source MAC address was copied.

1 16. The intermediate node according to claim 14, wherein:
2 the memory is further adapted to store an IP filter containing a list of IP addresses,
3 and
4 the network operating system is further configured to perform the steps:
5 parsing a destination IP address from the received data packet;
6 comparing the parsed destination IP address to one or more IP ad-
7 dresses stored in an IP filter associated with the shared media port; and
8 if the parsed destination IP address matches an IP address stored in
9 the IP filter, forwarding the received data packet over the first logical
10 subinterface's dedicated network or subnetwork, even if the first client
11 node is determined not to be authenticated to communicate over that net-
12 work or subnetwork.

1 17. The intermediate node according to claim 14, wherein:
2 the memory is further adapted to store a MAC filter containing one or more en-
3 tries configured to store at least a MAC address and an authentication state, and
4 the network operating system is further configured to perform the steps:
5 parsing a source MAC address from the received data packet;
6 indexing an entry in a MAC filter associated with the shared media
7 port based on the value of the parsed source MAC address;
8 identifying an authentication state stored in the indexed MAC-filter
9 entry; and
10 determining whether the first client node is authenticated to com-
11 municate over the first logical subinterface's dedicated network or sub-
12 network based on the authentication state stored in the indexed MAC-filter
13 entry.

1 18. An apparatus that implements port-based network access control at a shared me-
2 dia port, the shared media port being coupled to a plurality of client nodes, the apparatus
3 comprising:

4 means for partitioning the shared media port into a plurality of logical subinter-
5 faces, each logical subinterface dedicated to providing access to a different network or
6 subnetwork accessible through the intermediate node;

7 means for receiving a data packet at the shared media port from a first client node;

8 means for associating the received data packet with a first logical subinterface in
9 the plurality of logical subinterfaces;

10 means for determining whether the first client node is authenticated to communi-
11 cate over the first logical subinterface's dedicated network or subnetwork; and

12 means for forwarding the received data packet over the first logical subinterface's
13 dedicated network or subnetwork.

1 19. The apparatus according to claim 18, wherein the means for determining whether
2 the first client node is authenticated to communicate over the first logical subinterface's
3 dedicated network or subnetwork further comprises:

4 means for parsing a source MAC address from the received data packet;

5 means for indexing an entry in a MAC filter associated with the shared media port
6 based on the value of the parsed source MAC address;

7 means for identifying an authentication state stored in the indexed MAC-filter
8 entry; and

9 means for determining whether the first client node is authenticated to communi-
10 cate over the first logical subinterface's dedicated network or subnetwork based on the
11 authentication state stored in the indexed MAC-filter entry.

1 20. The apparatus according to claim 18, further comprising:

2 means for parsing a destination IP address from the received data packet;

3 means for comparing the parsed destination IP address to one or more IP ad-
4 dresses stored in an IP filter associated with the shared media port; and

5 means for forwarding the received data packet over the first logical subinterface's
6 dedicated network or subnetwork, even if the first client node is determined not to be
7 authenticated to communicate over that network or subnetwork.

1 21. The apparatus according to claim 18, wherein the means for associating the re-
2 ceived data packet with the first logical subinterface, further comprises:

3 means for locating an entry in a routing table configured to store routing informa-
4 tion associated with the received data packet; and

5 means for associating the received data packet with the first logical subinterface
6 based on the contents of the routing-table entry.

1 22. The apparatus according to claim 18, further comprising:

2 means for receiving an authentication request from the first client node at the
3 shared media port;

4 means for creating a MAC filter associated with the shared media port if the MAC
5 filter has not already been created;

6 means for copying a source MAC address stored in the received authentication
7 request into an appropriate entry in the MAC filter;

8 means for forwarding the received authentication request to an authentication
9 service;

10 means for receiving a response from the authentication service, the response
11 identifying an authentication state associated with the first client node; and

12 means for storing the authentication state into the same MAC-filter entry into
13 which the source MAC address was copied.

1 23. The apparatus according to claim 22, wherein the received authentication request
2 is an 802.1X authentication request.

1 24. A computer-readable media including instructions for execution by a processor,
2 the instructions for a method of implementing port-based network access control at a

3 shared media port in an intermediate node, the shared media port being coupled to a plu-
4 rality of client nodes, the method comprising the steps:
5 partitioning the shared media port into a plurality of logical subinterfaces, each
6 logical subinterface dedicated to providing access to a different network or subnetwork
7 accessible through the intermediate node;
8 receiving a data packet at the shared media port from a first client node;
9 associating the received data packet with a first logical subinterface in the plural-
10 ity of logical subinterfaces;
11 determining whether the first client node is authenticated to communicate over the
12 first logical subinterface's dedicated network or subnetwork; and
13 if the first client node is determined to be authenticated to communicate over the
14 first logical subinterface's dedicated network or subnetwork, forwarding the received
15 data packet over the first logical subinterface's dedicated network or subnetwork.